UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/603,424	06/24/2003	Branislav N. Meandzija	15685P208	3310

45222 7590 04/20/2006

ARRAYCOMM/BLAKELY
12400 WILSHIRE BLVD
SEVENTH FLOOR
LOS ANGELES, CA 90025-1030

EXAMINER	
ARANI, TAGHI T	

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 04/20/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/603,424	MEANDZIJA ET AL.	
	Examiner	Art Unit	
	Taghi T. Arani	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED. (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *24 June 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-48* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-48* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *24 June 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Taghi T. Arani
Primary Examiner
Au 2131
9/17/06

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-48 have been examined and are pending.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

2. Claims 8-9, 24-25, 40-41 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

The term "speculatively" in claim 8-9, 24-25, 40-41 is a relative term which renders the claim indefinite. The term " speculatively " is not defined by the claim, the specification does not provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would not be reasonably apprised of the scope of the invention.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later

invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

3. Claims are rejected under 35 U.S.C. 103(a) as being unpatentable over US patent 6,189,098 to Kaliski, Jr. and further in view of Persson et al., US patent 6,886,095 to Hind et al (hereinafter "Hind").

As per claims 1, 17 and 33, Kaliski, Jr. teaches a method , a user terminal and a machine-readable medium performed by a user terminal of a wireless access network, the method comprising:

generating a shared secret to be provided to an access point of the wireless access network (col. 4, lines 44-45, i.e. KSS||TS);

encrypting the shared secret with an access point public key (col. Col. 4, lines 39-55, i.e. {KSS||TS}PUBserv);

sending a message to the access point, the message including the encrypted shared secret, a user terminal certificate (col. 9, lines 8-12).

While Kaliski, Jr. teaches generating an authenticator (col. 10, lines 30-50, i.e. concatenating a time-varying value with the certificate and encrypting the result using the shared secret) Kaliski, Jr. does not teach but Hind teaches the authenticator string demonstrating possession of a user terminal private key and sending a message to the access point , the message including the authenticator string (col.12, lines 42-55).

It would have been obvious to one of ordinary skill in the art to modify the teachings of Kaliski, Jr. to include an authenticator string demonstrating possession the users terminal private key as taught by hind with a motivation that an imposter would not be able to impersonate the user terminal of Kaliski, Jr. by replaying the certificate in transmission (hind, col. 12, lines 55-62).

4. Claims 2, 18 and 34 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kaliski, Jr. as applied to claims 1, 17 and 33 above, and further in view of Persson et al., US patent 6,754,824 (hereinafter "Person").

As per claims 2, 18 and 34, Kaliski teach the method, the user terminal and the machine-readable medium of claims 1, 17 and 33 respectively, except wherein the user terminal certificate is scrambled, using a pseudo-random sequence generator initialized with a part of the shared secret, before being included in the message.

However, in an analogous art, Persson is directed to telecommunications systems and methods wherein the identity of the transmitting node is verified by modulating the CRC code utilizing a sequence known only to the participating parties. The modified CRC is generated by both the transmitting node and the receiving node initializing a LFSR register by a common key known only to the participating nodes (i.e. a pseudo-random sequence generated by a linear feedback shift register initialized with a part of the shared secrete (Persson, col. 2, lines 5-23).

Therefore, it would have been obvious to one of ordinary skill at the time the invention was made to employ the teachings of Persson within the method and system of Kaliski for combining Kaliski's certificate with a pseudo-random sequence generated by a linear feedback

shift register initialized with a part of the shared secret in order to verify both the authenticity of the received certificate and the identity of transmitting node and to deter unauthorized party to replace the participating nodes if week encryption or no encryption is switched on after authentication (Persson, col. 1, lines 35-49).

As per claims 3, 19 and 35, Kaliski Jr. The method, the user terminal and the machine-readable medium of claims 2, 18 and 34 respectively, wherein the remainder of the shared secret comprises a master secret to be used for symmetric key cryptography between the user terminal and the access point (col. 4, lines 42-55, i.e. KSS is used for symmetric key cryptography, the remainder of KSS||TS).

As per claims 4, 20 and 36, Kaliski, Jr. as modified teaches the method, the user terminal and the machine-readable medium of claims 1, 17 and 33, wherein generating the authenticator string comprises generating an authenticator message and signing the authenticator message with the user terminal private key (Hind, col. 12, lines 52-54).

As per claims 5, 21 and 37, Kaliski, Jr. as modified teaches the method, the user terminal and the machine-readable medium of claims 4, 20 and 36 respectively, wherein signing the authenticator message comprises:

generating a digest of the authenticator message; and encrypting the authenticator message digest with the user terminal private key (Hind, col. 12, lines 54-55, Hind uses SSL/TSL protocol in signing the authenticator string using the terminal private key). The examiner asserts that generating a digest and encrypting the message digest with the private key of signer (user terminal) is inherent in SSL/TSL protocol disclosed by Hind in that the SSL

protocol is designed to support a range of choices for specific security methods used for cryptography, message digests, and digital signatures.

As per claims 6, 22 and 38, Once modified , Kaliski, Jr. teaches the method, the user terminal and the machine-readable medium of claims 4, 20 and 36 respectively, , wherein the authenticator message comprises a time parameter and at least part of the shared secret (col. 10, lines 30-50, i.e. Kaliski, Jr.'s authenticator string (i.e. certificate concatenated with time-varying value)

As per claims 7, 23 and 39. Kaliski, Jr. teaches the method, the user terminal and the machine-readable medium of claims 6, 22 and 38 respectively, wherein the user terminal generates the authenticator string by speculatively incrementing the time parameter to a time when the message is to be sent to the access point (col. 4, lines 39-43, i.e. client generates a time-varying value (TS) to be used by server which changes with time, see also col. 6, lines 34-40).

5. Claims 10-16, 26-32 and 42-48 are rejected under 35 U.S.C. 103(a) as being unpatentable over US patent 6,189,098 to Kaliski, Jr. and further in view of Persson et al., US patent 6,886,095 to Hind et al (hereinafter "Hind").

As per claims 10 and 42, Kaliski, Jr. teaches a method, a machine-readable medium performed by an access point of a wireless access network, comprising:

receiving a message from a user terminal of the wireless access network (col. 4, line 56 through col. 5 line 10), the message containing a shared secret encrypted with an access point public key, a user terminal certificate, (col. 9, lines 8-18);

decrypting the shared secret using an access point private key (col. 9, lines 3-7);

Kaliski does not teach but Hind teaches authenticating the user terminal by checking the authenticator string using a user terminal public key included in the user terminal certificate to verify possession of the user terminal private key by the user terminal (Hind, col. 7, line 57 through col. 8, line 23, see also col. 6, lines 10-25).

It would have been obvious to one of ordinary skill in the art to modify Kaliski's certificate with Hind's user terminal certificate containing identification of user terminal and a user terminal public key corresponding to a user terminal private key, wherein the user terminal certificate is used to authenticate the user terminal with a motivation to couple Kaliski's certificate with both users of the terminal and the terminal in order to solve the prior art problems associated with users' certificates in enterprise situations where each application (user) as well as each device may require a different levels of security , requiring the ability to allow different levels of security accesses (Hind, col. 7, lines 12-24).

As per claims 11 and 43, Kaliski Jr. teaches the method and the machine-readable medium of claims 10 and 42 respectively, wherein the user terminal certificate is scrambled, and the access point unscrambles the user terminal certificate using the shared secret (col. 4, lines 39-55, Fig. 3A and associated text).

As per claims 12 and 44, Kaliski Jr. as modified teaches the method and the machine-readable medium of claims 10 and 42 respectively, wherein checking the authenticator string comprises decrypting the authenticator string using the user public key (Hind, col. 7, line 57 through col. 8, line 23, see also col. 6, lines 10-25, col. 12, lines 42-63).

As per claims 13 and 45, Kaliski Jr. as modified teaches the method and machine-readable medium of claims 12 and 45 respectively, wherein checking the authenticator string further comprises generating and authenticator message, generating a digest of the authenticator message, and comparing the authenticator message digest with the decrypted authenticator string (Hind, col. 12, lines 54-55, Hind uses SSL/TSL protocol in signing the authenticator string using the terminal private key). The examiner asserts that generating a digest and encrypting the message digest with the private key of signer (user terminal) is inherent in SSL/TSL protocol disclosed by Hind in that the SSL protocol is designed to support a range of choices for specific security methods used for cryptography, message digests, and digital signatures).

As per claims 14 and 46, once modified, Kaliski Jr. teaches the method and the machine-readable medium of claims 13 and 45 respectively, wherein the authenticator message comprises at least part of the shared secret (col. 9, lines 8-19, see also col. 10, lines 30-50).

As per claims 15 and 47, Kaliski Jr. teaches the method and the machine-readable medium of claims 10 and 42 respectively, wherein the user terminal certificate is signed by a certificate authority trusted by the access point (col. 4, lines 4-25, see also col. 5, lines 5-10).

As per claims 16 and 48, Kaliski Jr. teaches the method and the machine-readable medium of claims 10 and 42, wherein the shared secret is to be used for symmetric key cryptography between the access point and the user terminal (col. 4, lines 39-55, the shared secret session key KSS is used for symmetric key encryption between the client and the server).

As per claims 26, Kaliski Jr. teaches an access point comprising:

a receiver to receive a message from a user terminal, the message containing a shared secret encrypted by the user terminal with an access point public key, a user terminal certificate including a user terminal public key (col. 4, lines 56 through col. 5, line 10, Fig. 3b and associated text);

a processor coupled to the receiver to decrypt the shared secret using an access point private key (col. 4, line 59-60);

While Kaliski Jr. teaches a processor coupled to the receiver to decrypt the shared secret using an access point private key (col. 4, line 59-60), Kaliski Jr. does not teach authenticating the user terminal by verifying possession by the user terminal of the user terminal private key.

However, Hind teaches the user terminal certificate includes an identification of the user terminal and a user terminal public key which corresponds to user terminal private key, wherein the user terminal certificate is used to authenticate the user terminal by verifying possession by the user terminal of the user terminal private key (Hind, col. 12, lines 42-63).

It would have been obvious to one of ordinary skill in the art to Kaliski's method and system with the teachings of Hind to authenticate the user terminal by verifying possession by the user terminal of the user terminal private key with a motivation to provide assurance that the data has not been changed in transmission (Hind, col. 8, lines 12-23);

As per claim 27, Kaliski Jr. teaches the access point of claim 26, wherein the user terminal certificate is scrambled, and the processor is further to unscramble the user terminal certificate using the shared secret (col. 4, lines 39-55, Fig. 3A and associated text).

As per claim 28, Kaliski Jr. as modified teaches the access point of claim 26, wherein the processor verifies possession of the user terminal private key by decrypting the authenticator string using the user terminal public key (Hind, col. 7, line 57 through col. 8, line 23, see also col. 6, lines 10-25, col. 12, lines 42-63)

As per claim 29, Kaliski Jr. as modified teaches the access point of claim 28, the processor further verifies possession of the user terminal private key by generating an authenticator message, generating a digest of the authenticator message, and comparing the authenticator message digest with the decrypted authenticator string ((Hind, col. 12, lines 54-55, Hind uses SSL/TSL protocol in signing the authenticator string using the terminal private key). The examiner asserts that generating a digest and encrypting the message digest with the private key of signer (user terminal) is inherent in SSL/TSL protocol disclosed by Hind in that the SSL protocol is designed to support a range of choices for specific security methods used for cryptography, message digests, and digital signatures).

As per claim 30, Once modified, Kaliski Jr. teaches the access point of claim 29, wherein the authenticator message comprises at least part of the shared secret (col. 9, lines 8-19, see also col. 10, lines 30-50).

As per claim 31, Kaliski Jr. teaches the access point of claim 26, wherein the user terminal certificate is signed by a certificate authority trusted by the access point (col. 4, lines 4-25, see also col. 5, lines 5-10).

As per claim 32, Kaliski Jr. teaches the access point of claim 26, wherein the shared secret is to be used for symmetric key cryptography between the access point and the user

terminal (col. 4, lines 39-55, the shared secret session key KSS is used for symmetric key encryption between the client and the server).

Conclusion

Prior arts made of record, not relied upon:

US 2001/0048744 to Kimura.

US 2002/0174335 to Zhang et al.

US 2003/0139180 to McIntosh et al.

US 2003/0084287 to Wang et al.

US 2004/0010713 to Vollbrecht et al.

2004/0098588 to Ohba et al.

US 6,870,930 to Kim et al.

US 6,996,714 to Halasz et al.

GB 2 369 530 to Telephonaktiebolaget LM Ericson

EP 1 178 644 A2 to Nokia Inc.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Taghi T. Arani whose telephone number is (571) 272-3787. The examiner can normally be reached on 8:00-5:30 Mon-Fri.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Taghi T. Arani, Ph.D.
Primary Examiner
Art Unit 2131
4/17/2006